AMENDMENTS TO THE DRAWINGS

The attached "Replacement Sheet" of drawings includes changes to Figure 1. The attached "Replacement Sheet", which includes Figure 1, replaces the original sheet including Figure 1.

Attachment: Replacement Sheet

REMARKS

Claims 1-18 are now pending in the application. Applicant has amended claims 1, 8, 10 and 13, the drawings, the specification and the abstracts. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

PRIORITY

Applicant has enclosed a certified copy of the CN application as required by 35 U.S.C. 119(b) with this response.

DRAWINGS

The drawings stand objected to for certain informalities. Applicant has attached revised drawings for the Examiner's approval. In the "Replacement Sheet", Applicant has revised Figure 1 to clearly point out it refers to prior art.

REJECTION UNDER 35 U.S.C. § 112

Claims 8-18 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Applicant has amended the specification and the claims 8-9 and 13. Therefore, reconsideration and withdrawal of this rejection are respectfully requested.

REJECTION UNDER 35 U.S.C. § 102

Claims 1-7 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Frankel (U.S. Pat. No. 6,035,041). This rejection is respectfully traversed.

Frankel fails to anticipate an offline secret key distributor that distributes the first sub-secret-keys to each of the online secret share calculators and the second sub-secret-keys and equation combination representations thereof to each of the online secret share combiners. Frankel at best appears to discuss the key distributor distributes key shares to each of the agents which apply their individual key shares to an input for producing a signature.

The subject application, as recited in the amended claim 1, is directed to online secret share calculators that are used for making calculation based on the first sub-secret-keys pre-stored (corresponding to the key shares in Frankel) and online secret share combiners that are used to obtain a second sub-secret-key (corresponding to key shares in Frankel) in accordance with the result of the calculation made in the online secret share calculators and to make calculation based on the second sub-secret-keys.

Frankel fails to anticipate that each of the m online secret share combiners can compare t calculation results from the k online secret share calculators with the equation combination representations pre-stored upon receiving at least t calculation results, get a second sub-secret-key corresponding to the t calculation results, make a calculation based on the t calculation results and the second sub-secret-key corresponding to the t calculation results, and generate a digital certificate. Frankel at best appears to discuss that an output processor receives the partial results generated

by the active agents based on the key shares distributed and combines the partial results into an output by the output processor without using the key shares.

The subject application, as recited in the amended claim 1, is directed to online secret share combiners (corresponding to an output processor in Frankel) that use second sub-secret-keys (corresponding to a key share in Frankel).

Frankel at best appears to discuss that re-expressing the first function is in the form of a t-of-l system, l being a number of cryptographic processing apparatus configured to provide partial result, and t being a minimum number of a partial results needed to generate a final result. See, col 19, lns 31-32.

The claims are directed to m online secret share combiners each of which can compare t calculation results from the k online secret share calculators with the equation combination representations pre-stored upon receiving at least t calculation results, k being a number of online secret share calculators, m being a number of online secret share combiners, and t being a minimum number of online secret share calculators that provides calculation results needed to generate a digital certificate. The process is in a form of t-of-k and one-of-m system. The digital certificate will be generated by online secret share combiner as long as one online secret share combiners is operating.

Amended claim 1 differs from Frankel in: a system of the present invention has a two-layer secret share structure; the secret key is distributed into the first sub-secret-keys pre-stored in the online secret share calculators and the second sub-secret-keys pre-stored in the online secret share combiners; the online secret share combiner can find a second sub-secret-key corresponding to the calculation results from the online

secret share calculators; the digital signature is generated based on the first sub-secret-key and the second sub-secret-key. Frankel at best appears to discuss a detailed public-key cryptographic system and method. The secret key in Frankel is distributed into one kind of, not two kinds of agents such as the online secret share calculators and the online secret share combiner in the present invention.

Amended claim 1 enables a system to resist a conspiracy attack from a secret share calculator and a secret share combiner: even when the secret share calculator and the secret share combiner are both intruded, the secret key will not be leaked, because the system needs at least t secret share calculators and a secret share combiner to generate a digital signature.

In view of the foregoing, Applicant respectfully submits that claim 1 defines over the art cited by the Examiner. Likewise, claims 2-7, which depend from claim 1, define over the art cited by the Examiner. Thus, Applicant respectfully requests that the Examiner withdraw the rejections over 35 U.S.C. 102(b).

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action and the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner

believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: February 22, 2007 By: /Joseph M. Lafata/
Joseph M. Lafata
Reg. No. 37,166

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

JML/pfd